## 概述

现在有些存储类的芯片都有一个唯一 ID 的数据(以下简称 UID)在芯片内部。

UID 具备唯一性，也就是每个芯片的 UID 数据都不一样。 是芯片出厂之前就固化在芯片内的一段只读数据，不可以修改，也不可以复制到其他芯片。

我们可以使用 UID 来给产品进行加密，防止产品被非法复制(盗版)。

## 基本原理

使用芯片的 UID 为数据源，通过一定的加密运算，得到一串加密数据。 并将加密数据保存到芯片的存储区。

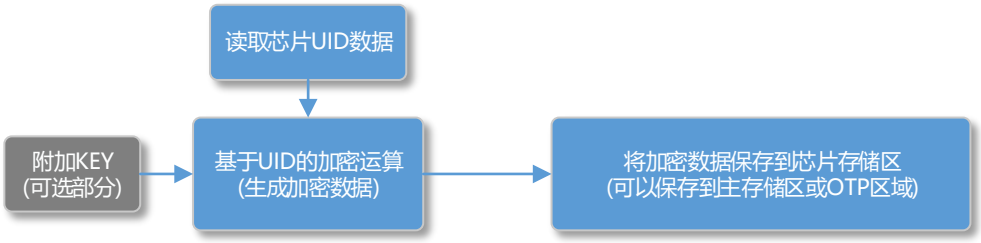
因每个芯片 UID 数据都不一样，那么加密数据也会不一样，这样一批产品中，每个芯片存储的内容都会不一样。 即任意一个芯片的内容(加密数据部分)只能与该芯片的 UID 匹配，如果有人将芯片内容复制到其他芯片，就会呈现加密数据与 UID 不匹配的情况。

因此: 我们可以在产品运行时,通过检查芯片的 UID 与加密数据是否匹配来判断产品是否为非法复制。

## 功能实现

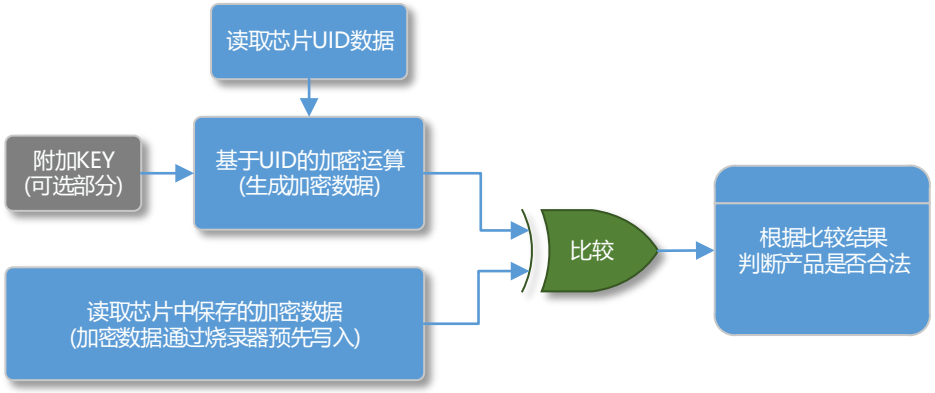
要实现 UID 加密功能，需要处理两个部分:

1. 在芯片中保存基于 UID 的加密数据，这部分可以在存储芯片烧录时通过烧录器完成。流程如下:




上述烧录操作可以使用硕飞的 SP328P 编程器完成。

2. 在用户产品运行时，检查 UID 与加密数据是否匹配，来判断产品是否合法。 流程如下:




注意: 产品运行代码使用的 UID 加密算法需与编程器一致。

# 硕飞 SP328P 编程器 UID 加密数据处理

硕飞的 SP328P 编程器提供了 UID 加密处理功能。

可以在烧录存储芯片时，根据当前芯片的 UID 生成加密数据，并写入到芯片中。

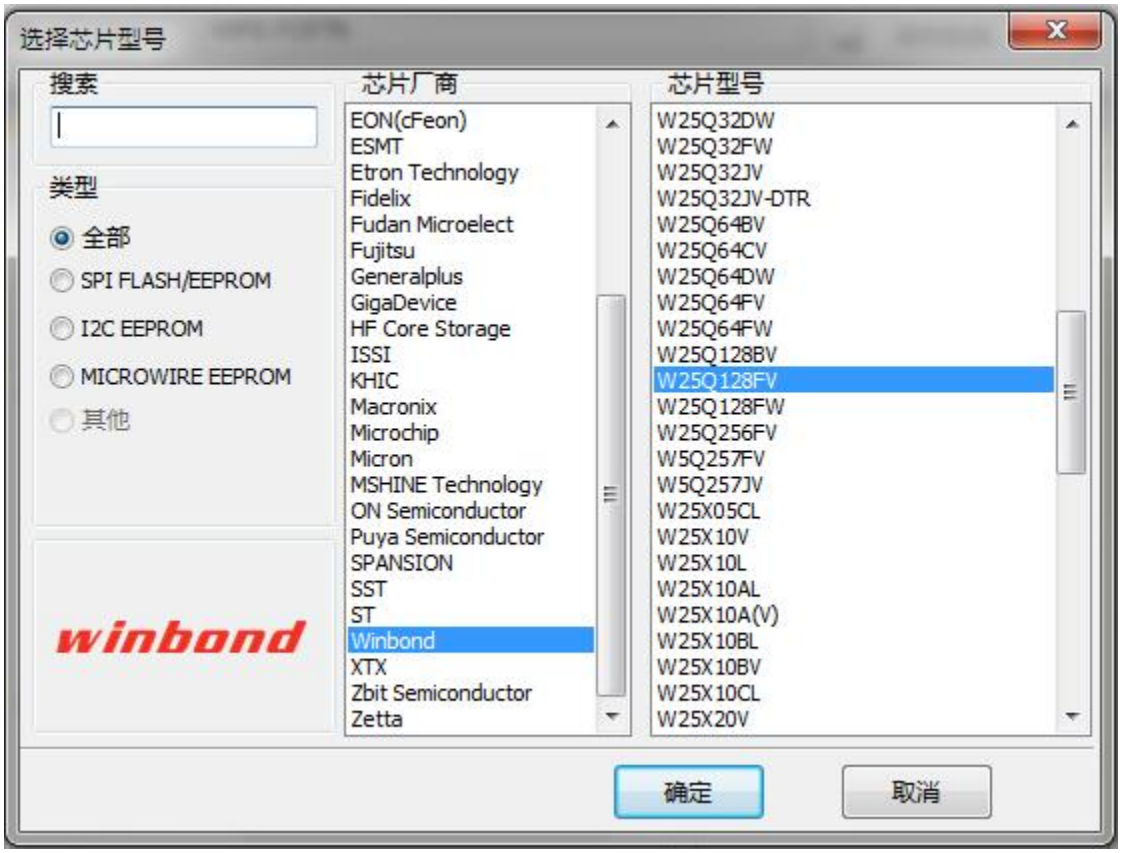
其内置有 SHA256 和 MD5 算法，可选额外的附加 KEY 参与加密运算。

加密数据可保存在芯片主存储区任何位置，由用户设置来指定；如果芯片具有 OTP 区域，也可以保存到 OTP 区域。

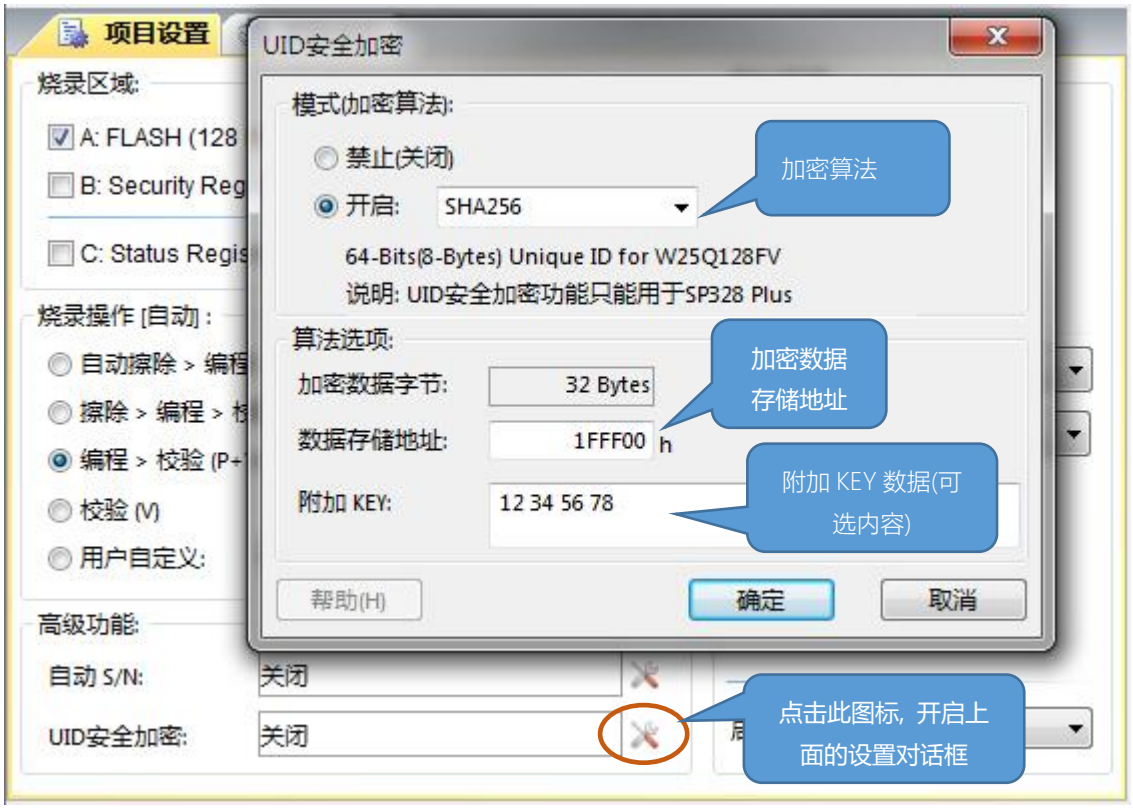
如果需要使用其他加密算法，还可以向硕飞定制软件。

**SP328P 编程器软件操作步骤**

1. 在软件中选带有 UID 型号(以 W25Q128FV 为示例)



2. 开启并设置 UID 安全加密功能



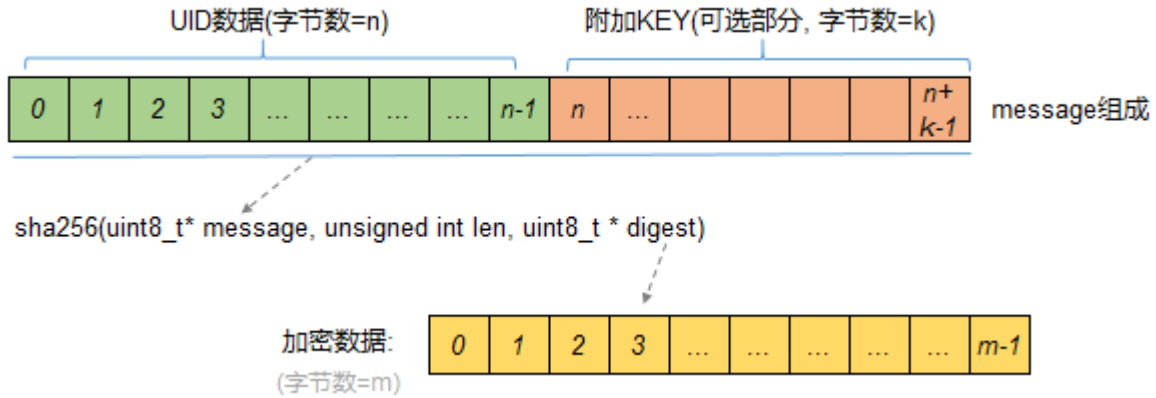

注意：上述数据存储地址为缓冲区映射地址，如果需要保存到芯片的 OTP 区域请在软件中打开芯片信息窗口查看 OTP 区域在缓冲区中的映射地址。

3. 经过上述设置，在烧录芯片时，编程器将自动读取芯片的 UID 并进行加密运算，并将数据保存到 0x1FFF00 开始的地方。

**关于附加 KEY**

软件提供附加 KEY 数据参与加密运算，这个是可选的内容，用户可以保留”附加 KEY”输入框为空白，则在加密运算时，不使用附加 KEY 参数。

当使用了附加 KEY 时，编程器将此参数附加在 UID 的后面进加密运算，以下是基于 SHA256 算法的示意图:




备注:

n 为芯片的 UID 数据字节数;

k 为用户输入的附加 KEY 字节数;

m 为生成的加密数据字节数，由算法类型决定（对于 SHA256 算法为 32 字节，MD5 算法为 16 字节）